IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:2006-31
	)	
JAMIE RICHARDSON,	)	JUDGE GIBSON
	)	
Defendant.	)	

MEMORANDUM OPINION and ORDER OF COURT

GIBSON, J.

Before the Court is the Defendant's Supplemental Motion to Suppress Evidence Obtained as a Result of an Unlawful Search and Seizure with Accompanying Citation of Authority (Document No. 83) filed on April 11, 2008. This motion was filed by the Defendant's current counsel, Adam Cogan, Esquire who was appointed by the Court on October 31, 2007. *See* Document No. 70. Without objection of the Government, Attorney Cogan was permitted to file the present motion after seeking permission from the Court to do so during a hearing on February 14, 2008. *See* Document No. 78.

An evidentiary hearing on the supplemental motion was held on June 2, 2008. The Defendant filed Proposed Findings of Fact and Conclusions of Law on July 24, 2008. *See* Document No. 97. The Government filed its Proposed Findings of Fact and Conclusions of Law and Post-Hearing Brief on August 22, 2008. *See* Document No. 101.

Pursuant to 18 U.S.C. § 3231, this Court possesses subject matter jurisdiction over the offense alleged: possession of material depicting the sexual exploitation of a minor. *See* 18 U.S.C. § 2252(a)(4)(B). Venue is proper in this court. *See* Fed. R. Crim. P. 18.

I. FINDINGS OF FACT

The Court sets forth both the findings of fact from its previous Memorandum Opinion and Order of Court (Document No. 51), now published as *United States v. Richardson*, 501 F.Supp 2d 724 (W.D.Pa. August 3, 2007)(*Richardson I*), and its supplemental findings of fact originating from the record produced as a result of the Supplemental Motion to Suppress. The supplemental findings of fact are set forth in bold accompanied by supplemental, alphanumeric numbering and inserted within the Court's previous findings in the most logical sequence. In a few instances, additional citations to the supplemental hearing transcript have been added to the previous findings of fact, the email address associated with the Defendant has been corrected throughout the original and supplemental findings of fact (*see* footnote one) and one finding of fact has been amended to correct a previous factual error it contained. *See* Finding of Fact ("FOF") 37 and footnote four, *infra*. Additional, non-substantive corrections and amendments of the original findings of fact are indicated in bold.

1. In July 2006, Special Agent Patricia Lieb (Lieb) of Immigration and Customs Enforcement (ICE), Pittsburgh Office, was assigned a case involving Jamie Richardson (Defendant) as a result of "Operation Emissary." Transcript (Document No. 43)("T."), p. 7.

1a. Special Agent James Kilpatrick (Kilpatrick), a "certified computer forensics examiner" has been employed with ICE since 2001 and was assigned to the Pittsburgh ICE Resident Agent in Charge in 2006. Supplemental Hearing Transcript (Document No. 95) ("S.T."), pp. 46-47.

2. "Operation Emissary" is the name for an investigation conducted by the Newark, New Jersey Office of ICE that concerned people who subscribed to or attempted subscription to an **Internet Web site** entitled "ILLEGAL.CP" which was a website that published child pornography; "CP" refers to child pornography. T., p. 8.

2a. Defendant's Exhibit A contains the informa tion provided to Lieb from Operation Emissary regarding the two attempts to access "ILLEGAL.CP" in January and February 2006 including the Defendant's name, physical address, his email address of

jamie_lee_r@yahoo.com, credit card number with its accompanying cvv number, bank name and expiration date, two Internet Protocol addresses and a telephone number that has not been disproven to belong to the Defendant. S.T., pp. 15-20, Defendant's Exhibit A.

2b. The two attempts to access the website reflected in the information at Defendant's Exhibit A are identical as to the identifying information of the Defendant with the exception of the two Internet Protocol addresses which differ. S.T., pp. 18-20; Defendant's Exhibit A.

3. As a result of information provided from the Newark ICE office, Lieb was aware that a person attempted subscribing to "ILLEGAL.CP" in January 2006 and February 2006 through the email address of "**jamie_lee_r@yahoo.com**". T., pp.8-9.[1]

4. Newark ICE believed this email address belonged to the Defendant who resided at 1529 Pitt Road in Altoona, Pennsylvania and had concluded that the computer from which someone had attempted the subscription had an Internet Protocol (IP) address that was registered to the Defendant at the same address. T., p. 9.

5. Also among the available evidence was information related to the credit card account that was used in the attempted subscription and such information revealed that no charge was reflected on the credit card account because the "credit card was not functioning at the time"; a credit card charge of $79.99 was necessary to access the website. T., pp. 9-10.

5a. The information gathered by ICE in Defendant's Exhibit A regarding the credit card number that was used in the attempts to access the Web site indicated that the credit card number was inactive. S.T., pp. 26-27, 44.

5b. The information from Newark ICE revealed that the Defendant was not successful in logging into the Web site and downloading any information. S.T., p. 44.

6. Lieb admits that the whole of this information which was received **from** Newark ICE did not establish that the Defendant or the person using "**jamie_lee_r@yahoo.com**" actually accessed the website in question, only that access was "attempted". T., p. 10.

6a. The Newark office of ICE contacted Verizon after determining that it was the Internet service provider for the two IP addresses in question. S.T., pp. 20-21.

---

[1]This email address has been changed in this Memorandum Opinion to jamie_lee_r@yahoo.com from its previously incorrect version set forth in the Memorandum Opinion of August 3, 2007.

6b. In response to a grand jury subpoena, Verizon produced what has been designated Defendant's Exhibit B, that is information regarding the activity for the two IP addresses in question. S.T., pp. 21-22.

6c. Following up on the information provided by ICE Newark, Lieb had a grand jury subpoena laid on the bank account numbers at First Commonwealth Bank reflected in Defendant's Exhibit A and the resulting information revealed that "[t]here were no charges to the bank account number." S.T., pp. 17-18.

6d. Lieb had no other information indicating attempted access to the Web site by someone other than the Defendant at the time she approached the Defendant on September 6, 2006. S.T., pp. 24-26.

6e. Lieb did not know prior to going to the Richardsons' residence if they used a "wireless router device" with their computer. S.T., p. 11.

7. Armed with this evidence, Lieb along with two other Pittsburgh ICE agents, Kenneth Rochford (Rochford) and **[Kilpatrick]**, decided to approach the Defendant at his residence and inquire further as to the credit card account in question and the Defendant's "activity over the Internet." T., pp. 11, 100-101.

8. Lieb did not apply for a search warrant prior to visiting the Defendant's **Web site** and personally did not believe probable cause existed to conclude child pornography was located on the computer in question because access to the **Web site** was never granted, but only attempted. T., pp. 11, 83.

9. On September 6, 2006, at "approximately 11:10 in the morning" Lieb, along with Rochford and Kilpatrick and a police officer from Logan Township, Blair County, Pennsylvania approached the Defendant's home at 1529 Pitt Road in Altoona, Pennsylvania. T., pp. 12, 80-81.

9a. On September 6, 2006 while accompanying Lieb, Kilpatrick was dressed in blue jeans and a polo shirt with his weapon holstered on his hip and "probably" had a jacket on that obscured the weapon from view. S.T., p. 48.

10. Lieb knocked on the Defendant's door, the Defendant answered, and then Lieb and Kilpatrick, who were standing "at the door" produced their identification and badges for the Defendant and indicated to him in a "causal, polite" tone that they would like to speak to him regarding "some [of his] credit card activity over the Internet and [they] were looking into it and would like to

talk to them[2] regarding that activity"; Rochford and the Logan Township police officer stood "off to the corner of the residence". T., pp. 12-15, 16, 62, 81.

10a. Initially it appeared to be a concern for the Defendant that the agents were present to address an issue with his wife because he inquired if their visit concerned her. S.T., pp. 83-84.

10b. Lieb was not aware that the Defendant's wife had a pending application for citizenship with the Department of Homeland Security at the time Lieb approached the Defendant's home in September 2006, but only learned of the application when speaking with the Defendant and his wife later that same day. S.T., pp. 8-9.

10c. Despite Kilpatrick's lack of knowledge regarding the immigration status of the Defendant's wife, he recalls that the Defendant, in response to the agents' presence at his door, inquired as to whether they had come to address an issue with the Defendant's wife. S.T., pp. 80-82.

11. The Defendant invited Lieb, Kilpatrick and Rochford into his home in order to speak to these agents regarding the Internet and his credit card activity; the Logan Township police officer departed from the residence at this time. T., pp. 13, 14.

12. Lieb was dressed "causally" that day, "with a windbreaker that said ICE on it", with her firearm at her waist, not drawn but holstered and obscured from view by her windbreaker.[3] T., p. 13.

13. Once inside the residence, Lieb repeated the purpose of her visit to both the Defendant and his wife while sitting at the "kitchen table"; in response, the Defendant and his wife recounted occurrences to Lieb and the other agents regarding possible past theft of their identities, "issues with their computer in Germany, as well as some mail that they had received and some other problems and issues with their credit cards at two different banks." T., pp. 15, 16, 17, 82-84.

14. In approaching the Defendant in his doorway and during the conversation in the Defendant's kitchen, Lieb did not indicate to the Defendant that she had the intention of "investigating the

---

[2]Apparently Lieb was referring to the Defendant and his wife, Gabrielle, collectively in this comment. Defendant's wife was the only other person in the residence at this time, but the Defendant's daughter came home later in the afternoon. T., pp. 15, 22, 71.

[3]Rochford was wearing "a pair of jeans and a polo shirt," and his "standard issue gray vest" and also possessed his firearm but never drew it. T., p. 82.

possibility that he was in possession of child pornography" although this was her intent when she arrived at the Defendant's home. T., pp. 16, 60, 63, 70, 82.

15. The only purpose of the agents in referring to the fact that someone had improperly used Defendant's credit card was to secure his cooperation; and the content of what was told to the Defendant was not false. T., pp. 101-102.

16. The Defendant and his wife provided documentation regarding "disputed...transactions with two different banks,...Commonwealth **Bank** and...Citizens Bank." T., p. 17.

17. The Defendant broached the subject of child pornography by informing the agents that he previously "had a problem with child pornography on his computer or over his e-mail in Germany" and had at that time "approached either the German or the FBI authorities or both while he was in Germany, that he cleaned out that computer and then he passed it on to his father-in-law." T., pp. 17-18, 90; **S.T., p. 49.**

17a. Lieb inquired of the Defendant as to what phone and Internet services and "account names he used" and "who had access to his computers" in his home, but she never asked him if he was signed onto his Internet service provider (Verizon) or attempted access to "ILLEGAL.CP"on the two instances in question and she never asked him "if he...had an interest in child pornography...." S.T., pp. 33-34, 35.

17b. Lieb never indicated to the Defendant that someone had attempted accessing the "ILLEGAL.CP" web site using his bank account, physical address, email address, IP addresses and the phone number. S.T., p. 36.

17c. Lieb "had no personal knowledge of any wireless technology being used [in the Defendant's home]". S.T., p. 39.

17d. Lieb did not recall asking the Defendant if he possessed any wireless technology for use in connecting to the Internet. S.T., p. 36.

18. The Defendant and his wife further offered in the discussion that certain occurrences, including previously unauthorized charges to their "credit cards and bank accounts" and a previous telephone call from a "telemarketer" may have resulted in theft of their identities. T., p. 19.

19. The Defendant and his wife initiated the discussion concerning identity theft and Lieb did not prevent the discussion regarding identity theft and considered it to be "a possibility of [her] investigation" in light of the fact that another suspected subscriber to "ILLEGAL.CP" had used a stolen credit card to access that website. T., pp. 19-20.

19a. The Defendant also broached the subject of his prior experience of discovering child pornography on a computer he owned before Kilpatrick requested consent to search the Defendant's computers. S.T., pp. 88, 102-103, 108.

20. The topic of identity theft was discussed before and after consent was provided to image the two hard drives; Lieb never told the Richardsons "that they may be subject to any type of criminal penalty". T., pp. 70, 98-99.

21. During this entire discussion, the Defendant never felt that he "[was] a suspect in criminal activity". T., pp. 113, 129.

22. Lieb made an inference to the Richardsons that they were victims of identity theft "throughout the entire time that [the agents] were there". T., p. 79.

23. While these aforementioned topics were discussed throughout the approximately four hours the agents were present in the Defendant's residence, it was approximately within fifteen minutes after Lieb had entered the Defendant's home that she requested the Defendant's "consent to image his hard drives". T., pp. 20-21, 30-31, 84-85, 96.

23a. Kilpatrick inquired as to the presence of any computers in the home and the Defendant indicated that there were two computers, lead Kilpatrick into "the back bedroom" where the Defendant revealed the two computers and indicated that one would not work while the other did. S.T., pp. 49, 103.

23b. Kilpatrick and the Defendant then left the bedroom and Kilpatrick made an oral request to "image" the hard disc drive of the Hewlett Packard computer and the Defendant orally consented; Kilpatrick retrieved a written consent form, returned to the back bedroom and recorded the computer's "biographical information", specifically the computer's serial number, on the consent form at Government Exhibit 1. S.T., pp. 49-50, 85-86, 103-104.

23c. Kilpatrick and the Defendant again walked out of the back bedroom into the kitchen and Kilpatrick once again orally requested permission to image the Hewlett Packard computer's hard disc drive and the Defendant consented by executing the consent form and had no questions for the agents after being asked by them if he had questions regarding the consent form. S.T., pp. 49-51, 103-104; Government Exhibit 1.

23d. The Defendant did not appear to Kilpatrick to have been under the influence of alcohol or controlled substances or to have been otherwise ill when he granted consent to search and reviewed the consent to search form; the Defendant demonstrated no difficulty in understanding or communicating with Kilpatrick when granting consent. S.T., pp. 104-105.

23e. Lieb confirmed that consent to image the computers was obtained orally before written consent was given by the Defendant; the Defendant did not express any limitations that were to be placed on the consented imaging. S.T., pp. 12-13.

24. The Defendant agreed in writing to the requested search of two computer hard drives in his possession as found in Government Exhibits 1 and 2, both of which are forms entitled "CONSENT TO SEARCH COMPUTER(S)"; these forms were presented to the Defendant by Kilpatrick and Mrs. Richardson witnessed the Defendant's signature on Government Exhibit 1 and Lieb witnessed the signature on Exhibit 2. T., pp. 22-23, 116-117, 128.

25. Kilpatrick had filled in the information in the blank spaces of the consent forms with the exception of the date, signature and address lines on the bottom half of the form. T., pp. 23-25.

26. The Defendant examined the two forms and appeared to have read both forms; no agent read aloud the contents of the forms to the Defendant; after reviewing each of these forms, the Defendant asked questions regarding the need to remove the computers from the home in order to conduct the search and Lieb answered these questions. T., pp. 23, 58-59, 76-77, 85-86.

27. The Defendant was never read his ***Miranda*** rights as Lieb believed the conversation to be "a consensual encounter." T., p. 32.

28. Government Exhibits 1 and 2 were not presented to the Defendant at the same time; Lieb informed the Defendant that he could refuse the requested consent and her request was presented in a "polite agreeable voice"; neither Lieb nor Rochford threatened the Defendant or promised something to him, or otherwise exhibited a firearm or "physically touch [ed]" the Defendant in an attempt to secure his consent. T., pp. 24, 26, 27, 87.

29. Lieb indicated that the purpose of searching the hard drives was to search "[f]or Internet activity" but she did not describe to the Richardsons which "violation of law" she was investigating. T., p. 32; Government Exhibit 2.

30. The Defendant did not appear to be under the influence of any alcohol or illegal substance at the time of providing his consent and the Defendant's responses to questions, while at times "stray[ing] from the direct question" were "responsive." T., pp. 28, 92.

31. Lieb admits that "[i]n some definitions for a ruse-I may have used a ruse in the initiation of the interview" and described her tactic as such: "I explained to him that there was some credit card activity over the Internet and it was his credit card, however, I didn't explain exactly what it was for, what the activity was or the website that was accessed." T., pp. 28-29.

32. Although Rochford did not believe Lieb's tactic was a ruse, he agreed that the Defendant was only told that his credit card may have been used for "illegal activity" over the Internet by "someone", but was never told that what the "illegal activity was". T., pp. 92-94, 98.

33. Lieb's statement to the Defendant regarding "illegal activity" was true, but was not complete in that it did not describe Operation Emissary or Lieb's knowledge about all of the facts concerning the Defendant's attempted credit card and computer use. T., pp. 28-30.

33a. From what little he heard of the conversation between the Defendant and Lieb inside the home, Kilpatrick does not recall that Lieb told the Defendant that the investigation concerned child pornography. S.T., p. 85.

34. The subject of "identity theft" was initiated by the Richardsons and brought up prior to and after the Defendant granted his consent reflected in Government Exhibits 1 and 2. T., pp. 30, 32, 99-100.

35. Lieb did use the word "victim" during her conversation with the Richardsons, but not prior to requesting consent to image the hard drives. T., pp. 74, 78, 88, 113.

36. The Defendant believed the forms were being presented to him in an effort to help the agents investigate the possibility of the Defendant being a victim; the Defendant contends that he signed them without "car[ing] about reading them". T., pp. 113-114, 116-117.

36a. Kilpatrick was not aware of any restrictions to his forensic search; Kilpatrick had explained to the Defendant that "we needed to look at the computer to find out how these charges and allegations occurred." S.T., p. 51.

37.[4] After consent was provided by the Defendant, Kilpatrick, a computer forensic investigator, "image[d]" the hard **drive of the Hewlett Packard computer** owned by the Defendant; to "image" means to "mak[e] a duplicate of the hard drive...so that anything that is on that hard drive could not be corrupted or changed, it would make a copy of it and then he would look at that copy." T., pp. 21-22, 26, 88-89; **S.T., pp. 51-52, 55.**

37a. Kilpatrick did not conduct an onsite preview of the contents of the hard drive of the Hewlett Packard computer but only imaged it in order to obtain an exact copy of its contents, but a forensic review of the contents was conducted back at Kilpatrick's forensic lab in Pittsburgh. S.T., pp. 51-52, 54, 86-87.

---

[4]This finding of fact previously indicated that images were made of both computers hard disc drives, but that was incorrect as only the Hewlett Packard was imaged on September 6, 2006 and the Nascar PC by CISNET was physically removed from the Defendant's possession for analysis of its hard disc drive. *See* FOF 41, *infra.*

38. The hard drives were never physically removed from the Defendant's residence during the conversation. T., p. 22.

39. During the course of the imaging of the Hewlett Packard hard drive, a period of at least three hours but not more than five hours, the Defendant and his wife were interviewed by Lieb and Rochford at the kitchen table of the residence; the parties took occasional breaks but at no time did the Defendant rescind his consent, end the interview, request an attorney or direct the agents to leave his home and for the duration he remained "cooperative." T., pp. 32-33, 88-89, 91, 98, 115, 129.

40. The Richardsons provided to the agents all their bank statements they had received since returning to the United States in April 2004 in an effort to facilitate what the Defendant believed to be **an investigation into the** theft of his identity. T., p. 114.

41. After the imaging of the Hewlett Packard hard drive was complete, *see* Government Exhibit 1, rather than await a second imaging, the agents requested permission to physically remove the second hard drive found in the Nascar PC by CISNET from the Richardson's home in order to review its contents in the agents' Pittsburgh office and the Richardsons consented to this action. T., p. 33; **S.T., p. 55.**

41a. In order to remove the Nascar PC by CISNET from the Defendant's home and take it back to ICE headquarters to analyze it, Kilpatrick offered the consent to search form found at Government Exhibit 2 that permitted that computer's removal from the home and a search of it by ICE. S.T., pp. 55-56.

41b. The Defendant signed the consent to search form at Government Exhibit 2 after appearing to read the form and without posing any questions to the agents. S.T., p. 56.

41c. Kilpatrick processed both the images retrieved from the Hewlett Packard computer and the Nascar PC by CISNET using a program named Forensics Toolkit, which despite possessing the capability of limiting the search conducted, was not limited in its search in this instance because Kilpatrick believed the search was without limitation. S.T., pp. 57-58.

41d. Kilpatrick also testified to the typical operation of wireless Internet connections whereby personal computers, laptop computers and even printers could operate and exchange information using a wireless router. S.T., pp. 60-65.

41e. According to Kilpatrick, an individual with a laptop that possesses wireless communication capabilities can access a wireless Internet network originating in another's residence that emanates from a wireless router because many residences do not protect

their wireless network by passwords. S.T., pp. 62-63.

41f. As explained by Kilpatrick, wardriving is the practice of an individual using wireless computer technology to locate and utilize another's wireless Internet service purchased by another party without the permission or knowledge of that party. S.T., p. 91.[5]

41g. Kilpatrick also offered that individuals usually within 1000 feet of the residence may use a "strong" wireless Internet connection signal originating within that residence (assuming the person outside had wireless capabilities on his computer). S.T., pp. 63-64.

41h. Someone who does access a residence's wireless Internet signal from outside of the residence would appear to the resident's Internet service provider as being someone within the residence and that resident's Internet protocol address would be associated with the Internet activity engaged in outside of the residence. S.T., pp. 64-65.

41i. The presence of a wireless router within a residence is not something that is associated with an Internet account, that is to say it is not reflected on the description of the service provided by the internet service provider. S.T., pp. 66.

41j. Kilpatrick did not know prior to entering the Defendant's residence if the Defendant possessed wireless Internet technology/capabilities with any computer that may have been in his home. S.T., p. 101.

41k. Kilpatrick was not aware of whether or not any wireless computer technology was within the Defendant's residence prior to September 6, 2006. S.T., p. 69.

41l. Kilpatrick acknowledged the fact that he did not investigate the possible locations from which a potential wireless Internet signal from the Defendant's home could have been wardriven, including the surrounding homes. S.T., pp. 93-95.

---

[5]*See also* http://www.webopedia.com/TERM/w/wardriving.html defining wardriving as "[t]he act of driving around in a vehicle with a laptop computer, an antenna, and an 802.11 wireless LAN adapter to exploit existing wireless networks." It has been recognized by one source that the act of wardriving is separate from the act of piggybacking in that wardriving is the actual search of the wireless Internet signal, while piggybacking is the act of using the signal. Piggybacking (internet access) http://en.wikipedia.org/wiki/Piggybacking_(internet_access) (Last visited Oct. 23, 2008); *See also* http://www.nytimes.com/2006/03/05/technology/05wireless.html?ei=5089&en=de3c127408552e0a&ex=1299214800&pagewanted=print (describing anecdotal evidence of piggybacking in metropolitan areas). For purposes of this Memorandum Opinion, the Court will use the term "wardriving" to mean both the search for and the use of another's wireless Internet signal without permission of the individual who purchased the signal.

41m. Kilpatrick did not recall observing any wireless technology or devices that were being utilized in the Defendant's home on September 6, 2006. S.T., p. 99.

42. The agents left the Richardsons' home at "approximately 4:45 p.m." Lieb indicated to the Defendant "[t]hat [ICE] would continue the investigation into the credit card use online and the Internet activity, and [they] would see what [they] could get off the computers and [they] would be in touch and/or [the Defendant] could be in touch with me." T., pp. 33, 73, 77.

43. Subsequently, Kilpatrick did a forensic analysis on both hard drives from the Richardson home which revealed "over 3,000 images of child pornography or suspected child pornography, as well as 11 video[s]." T., p. 34.

43a. In investigating the possibility of identity theft, Kilpatrick's forensic examination of the Hewlett Packard hard disc drive began with processing the hard disc drive with the Forensic Toolkit software and thereafter searched the results for images of child pornography. S.T., pp. 59-60, 88-90.

43b. Kilpatrick described his reasoning for searching the forensic results for images first: "Q. And child pornography was the first evidentiary bit of value that you found on the imaged hard drive; isn't that correct? A. Because that was the most efficient thing to look for to find out whether or not somebody within the house or somebody outside of the house had perpetrated this offense." S.T., p. 90.

43c. In contrast, Kilpatrick later in his testimony described his role in the investigation as follows:

> **I would say that I was part of the investigating team in this case to provide forensic support in the event that Mr. Richardson provided consent to search his computer. Then later, as a computer forensic examiner, my job was to examine the contents of the two computers that we had consent to search for to find out whether or not there was evidence that that credit card had been used from a computer in that house to access child pornography.**

S.T., p. 96 (emphasis added).

43d. After uncovering the child pornography on the computers' hard disc drives, Kilpatrick's investigation continued in an effort to ascertain the identity of the individual who used the computers to access the child pornography. S.T., pp. 66-67, 106.

43e. To determine who had been accessing the child pornography, Kilpatrick reviewed the various "user profile[s]" and "file structure[s]" of the hard disc drives. S.T., pp. 66-67.

43f. Some of the pictures were located in a computer file entitled "mine" and Kilpatrick's analysis of the use of the user profiles on the computers other than the Defendant's profile indicated to Kilpatrick that the Defendant was the computer user who downloaded the images. S.T., pp. 107-108.

44. From the portions of this material that Lieb viewed, she concluded that all children depicted in the photos and videos were under the age of eighteen. T., p. 34.

45. Lieb later had "at least two... **possibly** three" telephone conversations with the Defendant with Lieb and the Defendant each initiating at least one of the conversations; the conversations concerned the Defendant's concern for "some mail that he thought was of suspicious nature", and "on another occasion [Lieb and the Defendant] made arrangements to meet [in Lieb's] office" and finally they spoke about "further credit card transactions and disputes and some information [the Defendant] had regarding those disputes that he wanted to give [Lieb]." T., pp. 35-36.

46. During the second telephone conversation, Lieb indicated to the Defendant that she wanted to meet with him again and requested that he come to her Pittsburgh office and Richardson willingly agreed to do so, indicating that he could be in Pittsburgh on September 22, 2006 when his wife had to attend an appointment regarding her "immigration status"[6] in the same office building. T., pp. 36-37, 38, 39.

47. Lieb requested that the Defendant bring the hard **disc** drive from the Hewlett Packard, which was previously imaged at his residence, to Pittsburgh on September 22, 2006 for their meeting and the Defendant indicated that he would do so; Lieb never indicated why she wanted the Defendant to bring the **hard disc** drive to their meeting, but she believed from the review of the imaged copy of that hard **disc** drive, that the actual drive contained child pornography. T., pp. 37-38.

48. The Defendant "voluntarily" arrived at Lieb's office at "[a]pproximately noon" and Lieb met the Richardsons in the building's lobby and escorted the Defendant up to the third floor of the building into a visitor conference room because access to the third floor is restricted from the public by a separate elevator. T., pp. 39-40, 74, 115.

---

[6]Gabrielle Richardson is originally from Germany and was in the process of applying for residency in the United States. T., pp. 36-37, 111, 126.

48a. Members of the public seeking to enter the third floor of the ICE building in Pittsburgh must be escorted after passing through a metal detector. S.T., p. 43.

49. After arriving in the conference room, the Defendant gave Lieb the documents concerning the "disputed transactions" he previously mentioned as well as the Hewlett Packard hard **disc** drive; subsequent to receiving these items, Lieb told the Defendant that "numerous images of child pornography" were found on the two hard **disc** drives in question to which the Defendant responded with "surprise." T., pp. 40, 41, 115, 138.

50. Lieb did not administer *Miranda* warnings to the Defendant because despite her questioning, she did not attempt to place him in custody as she told "him he was not under arrest" and told him on "several" "occasions" "he was free to leave" "at any time." T., pp. 40-41.

51. The Defendant voluntarily proceeded to state that any child pornography could only have gotten on the heard drives through his actions and not someone else's actions, but the Defendant did not admit to storing the images intentionally but initially indicated that they may have been mingled with emails and websites that contained adult pornography and that he may have unintentionally opened the images and "immediately closed" them. T., pp. 41-42.

52. However, "as the interview progressed [the Defendant] said well, he may have opened the child pornography image." T., p. 42.

53. Lieb offered the Defendant restroom breaks and drinks; Lieb was dressed casually and conversed with the Defendant without "rais[ing] [her] voice or yell[ing] at him", and without making any threats or promises or touching the Defendant and did not have her weapon in her possession during the course of the interview. T. pp. 42-43, 45, 46.

54. During the interview the Defendant voluntarily wrote a statement under oath on "Customs Form 4604B" and "4604C", initialing the first page and signing the second and Lieb also signed the second page-this statement has been introduced as Government Exhibit 3. T., pp. 43-44, 133.

55. Lieb did not direct the Defendant what to write in this statement. T., p. 133.

56. The statement reflected in Government Exhibit 3 indicates that the Defendant believed the child pornography was placed on his hard drives when he attempted to view what he believed to be adult pornography. T., pp. 44-45.

57. The first interview between Lieb and the Defendant lasted from approximately "noon to about 1:50 [p.m.]" when the Defendant voluntarily left this interview at his request to join his wife downstairs in the same building so she could "put in her [residency] application" and he then indicated that he wanted to continue the interview with Lieb after he was finished with his

wife's residence affairs. T., pp. 37, 45-46, 134.

58. Lieb honored the Defendant's request to end this interview; the Defendant made his request at 1:50 p.m. T., pp. 133-134.

59. The statement set forth in Government Exhibit 3 was written by the Defendant "just minutes before he left." T., p. 137.

60. After approximately forty-five minutes, at 2:45 p.m., the Defendant returned to the third floor and stated to Lieb that he had "spoke[n] to his wife [outside of the building] and told her about the child porn being on his computer, and that she was surprised and upset...but that there's some things that he wanted to tell [Lieb] and to correct his statement." T., pp. 46-47, 130-131, 139.

61. Lieb lead the Defendant back into the conference room along with **Special** Agent Michael Opferman (Opferman) and began a second conversation with the Defendant; Lieb did not have her firearm with her, she was dressed casually and did not advise the Defendant of his ***Miranda*** rights at this time and indicated to him "that he could leave at any time" and "that he was not under arrest." T., pp. 45, 48, 103-104, 106.

62. Opferman, who was unarmed, never threatened or promised "anything" to the Defendant and did not come in physical contact with Defendant and never "raised [his] voice" to the Defendant. T., p. 107.

63. In this second interview of September 22, 2006, the Defendant admitted to saving the child pornography on his computers' hard **disc** drives because "he did not look at child pornography because he was interested in little girls but because he was looking for the mindset that was involved in people that looked at child pornography, why they looked at it"; in support of this contention, the Defendant indicated "that his niece had been molested as a young girl and he was curious." T., p. 49.

64. The second interview continued "between one hour and five minutes and one hour and fifteen minutes"; the Defendant was "offered food or drink [and] use of the restrooms." T., p. 49.

65. Lieb was seated and used a "tone of voice" that was "polite and conversational" during this interview as she never yelled or "rais[ed] [her] voice to the Defendant as he was "polite" and "cooperative"; the Defendant did not "appear to be under the influence of any drug or alcohol" during this interview and had no difficulty communicating and never indicated that he wished to stop the interview or speak with an attorney. T., pp. 50, 55.

66. As a result of the second interview, the Defendant voluntarily made a second, two page statement under oath, signed by the Defendant and witnessed by Opferman and also signed by Lieb found in Government Exhibit 4, which reflects the stated intent of the Defendant in viewing child pornography in an attempt to understand why persons take advantage of children in that way; the Defendant indicated that he believed that of all of the pornography on the hard **disc** drives "1/4 [is] child porn." Government Exhibit 4; T., pp. 51-52, 105, 134-135.

67. Lieb did not tell the Defendant "what to write...[o]n the second statement"; the statement was "compos[ed]" by the Defendant "throughout the interview" and he began to do **it** "shortly after he came back into [the ICE] office". T., pp. 135, 137.

68. During the second interview, the Defendant also remarked to Lieb that in regard to her arriving at his residence on September 6, 2006 and his possession of child pornography, "I had an idea that's why you guys were there." T., p. 56.

69. The Defendant also indicated to Lieb that he does not recall "access[ing]" an image that apparently was obtained on the morning of September 6, 2006; the Defendant also revealed that he would view the child pornography "three to four times a week" and "they were little girls between ages of 10 and 16 years of age." T., p. 57.

70. It was confirmed that the female minors depicted on the computer files were "between the ages of [ten] and [sixteen] years old." T., p. 135.

71. The second interview concluded at "[a]pproximately 4:00 [p.m.]" and the Defendant was permitted to leave, was not arrested, and was told that Lieb would be contacting him regarding "any further developments regarding the child pornography on his computer." T., pp. 53, 107.

72. The "next contact" Lieb had with the Defendant was when she arrived at his residence on October 12, 2006 accompanied by "ICE Special Agent James Stitzel [(Stitzel)] and a Logan Police Department Officer" to place the Defendant under arrest. T., p. 54.

73. The Defendant was "advised" of his ***Miranda***[7] rights through Lieb's reading of a preprinted form found at Government Exhibit 5, to which the Defendant responded that "he understood his rights" and that he did not wish to speak to Lieb without an attorney and then requested legal counsel; Lieb noted the Defendant's response and request on Government Exhibit 5 and no "further conversation" occurred between the Defendant and Lieb. Government Exhibit 5; T., pp. 54-55.

---

[7]*Miranda v. Arizona*, 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed.2d 694 (1966).

II. CONCLUSIONS OF LAW

A. Application of the law of the case doctrine

The Defendant has presented further argument regarding the issue of consent by the Defendant, particularly the nature of its voluntariness and the scope of the consent given. The Government has argued for the application of the law of the case doctrine to limit reconsideration of matters previously decided in the Memorandum Opinion addressing the first motion to suppress filed by the Defendant's former counsel.

> The law of the case doctrine "limits relitigation of an issue once it has been decided" in an earlier stage of the same litigation. *In re Continental Airlines, Inc.*, 279 F.3d 226, 232 (3d Cir.2002). We apply the doctrine with the intent that it will promote finality, consistency, and judicial economy. *In re City of Philadelphia Litig.*, 158 F.3d 711, 717-18 (3d Cir.1998). Reconsideration of a previously decided issue may, however, be appropriate in certain circumstances, including when the record contains new evidence. *Id.* at 718; *Bridge v. United States Parole Comm'n*, 981 F.2d 97, 103 (3d Cir.1992). This exception to the law of the case doctrine makes sense because when the record contains new evidence, "the question has not really been decided earlier and is posed for the first time." *Bridge*, 981 F.2d at 103. But this is so only if the new evidence differs materially from the evidence of record when the issue was first decided and if it provides less support for that decision. *In re City of Philadelphia Litig.*, 158 F.3d at 720. Accordingly, if the evidence at the two stages of litigation is "substantially similar," or if the evidence at the latter stage provides more support for the decision made earlier, the law of the case doctrine will apply. *Id.*

Hamilton v. Leavy, 322 F.3d 776, 786 -787 (3d Cir. 2003). The doctrine has also been recognized to permit a court to depart from an earlier ruling to otherwise change its previous ruling "if convinced that it is clearly erroneous and would work a manifest injustice."*Arizona v. California*, 460 U.S. 605, 619 n. 8 (1983) (citation omitted). More specifically, the Third Circuit has recognized that

> the law of the case doctrine does not restrict a court's power but rather governs its exercise of discretion. *Public Interest Research Group of New Jersey, Inc. v. Magnesium Elektron, Inc.*, 123 F.3d 111, 116 (3d Cir.1997). Accordingly, we have

> recognized that the doctrine does not preclude our reconsideration of previously decided issues in extraordinary circumstances such as where: (1) new evidence is available; (2) a supervening new law has been announced; or (3) the earlier decision was clearly erroneous and would create manifest injustice. *Id.* at 116-17.

In re City of Philadelphia Litigation, 158 F.3d 711, 718 (3d Cir. 1998). The law of the case doctrine has been recognized by the Third Circuit in at least one published criminal matter. *See United States v. Kikumura*, 947 F.2d 72, 77 (3d Cir. 1991).

The supplemental findings outlined in bold above with supplemental, alphanumeric numbering present findings of fact that were not previously found by the Court and that are now relevant to the issues of consent addressed in the Defendant's Supplemental Motion to Suppress. The Court considers these findings new evidence that permits it to address the circumstances of the search performed upon the Defendant's computers, but our review of the search conducted is limited by our previously rendered conclusions of law. To the extent that the Government argued that this Court previously ruled upon the matters concerning the scope of the search, *see* Government's Response, (Document No. 89), p. 15, the Court disagrees and notes the Government's position stated at the time of the evidentiary hearing: "We can talk about scope of consent because that really wasn't fully litigated and the Court didn't specifically rule on the scope of consent. But the voluntariness of the consent has now become the law of the case." S.T., p. 6 Furthermore, footnote five of the Government's "Proposed Findings...." (Document No. 101), which references Conclusion of Law 22 from *Richardson I*, does not stand for the proposition that the scope of the consensual search was previously ruled upon. Conclusion of Law 22 should be read in context with those conclusions of law preceding and following it:

> 18. Lieb's act of seeking and obtaining consent from the Defendant to search the two computers in his residence was in fact part of a ruse in that she permitted the Defendant

to believe that he was a victim of a crime when in fact she believed him to be a suspect of a crime.

19. In this sense, the case *sub judice* differs from *Brown, supra* in that *Brown* was read his rights and was questioned "regarding several unsolved murders." *Brown* at 956.

20. While Lieb suspected that the Defendant possessed child pornography, she did not believe she possessed evidence sufficient to establish probable cause of that fact and still harbored the thought that the Defendant was not the person who attempted to access the child pornography website, although her belief in such a conclusion was not as strong as her belief in the conclusion that the Defendant did in fact attempt the access of "ILLEGAL.CP".

21. As a result of Lieb's failure to discount the Defendant's belief that he was a victim of a crime, Lieb was given the Defendant's voluntary consent to search his computers for evidence that he was indeed a victim of a crime.

22. In light of the fact that Lieb could not confirm or deny the presence of child pornography on the computers in question or that the Defendant was a victim of a crime, the Defendant's consent granted to ICE was not akin to a warrantless search based upon a fabrication of a crime as in *Phillips* or otherwise a warrantless consent that permitted viewing of matters beyond the "very purposes contemplated by the [owner]" as in *Lewis, supra.*

23. By comparison, if Lieb arrived at the Defendant's home and indicated to him that a crime was committed by another person, when in fact no such crime occurred, and she used that indication to otherwise gain entry into the Defendant's home and gain his consent to search his computers and other effects, such a scenario would be the equivalent of the suggestion of the occurrence of a burglary in Phillips that permitted law enforcement's entry into a building without a search warrant and while knowing that a burglary did not occur.

Richardson I at 735 -736. (emphasis added). These conclusions of law discuss the manner in which consent was obtained voluntarily in comparison to those instances where the ruses used by law enforcement to conduct a search are not permissible under the Fourth Amendment. The reference in Conclusion of Law 22 to *Lewis*, is to the Supreme Court case of *Lewis v. United States*, 385 U.S. 206 (1966) wherein our quotation when read in context does not support the Government's contention that

a warrantless general search is permitted:

> But when, as here, the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business, that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street. A government agent, in the same manner as a private person, may accept an invitation to do business and may enter upon the premises for the very purposes contemplated by the occupant. Of course, this does not mean that, whenever entry is obtained by invitation and the locus is characterized as a place of business, an agent is authorized to conduct a general search for incriminating materials; a citation to the *Gouled* case, *supra*, is sufficient to dispose of that contention.

Lewis v. United States, 385 U.S. 206, 211 (1966). If anything, Conclusion of Law 22 must be read to stand for the proposition that the scope of a search is limited by the objective circumstances under which consent is provided. Nevertheless, Conclusion of Law 22 was written to address the fact that consent was voluntary, not to address the limits of its scope. Specifically, it addressed the fact that Lieb's vague explanation for the purpose of her visit on September 6, 2006 was not a lie or otherwise a misrepresentation, but in fact suggested to the Defendant that he was a victim of a crime and that Lieb understood that this was a possible explanation for the attempted subscription to "ILLEGAL.CP". In the absence of any misrepresentation, the consent obtained by Lieb was voluntary. However, as explored further herein, the Court concludes the subsequent search by Kilpatrick went beyond the scope of that permitted by the Defendant similar to the hypothetical undercover agent in *Lewis* who enters to purchase controlled substances, but then begins searching for matters beyond that permitted in the invitation to his undercover character.

Considering all of the circumstances, including the Government's comments on the record at the evidentiary hearing that it does not object to a review of the scope of the consent given by the Defendant as it believes that the issue of the scope of consent was not addressed in the prior motion to

suppress, the Court will proceed with a review of the scope of the consent. S.T., p. 6.[8] However, the Government's understanding is that "voluntariness of the consent has now become the law of the case." *Id.*

Indeed, the Court rendered the following conclusions of law in its previous opinion in this matter:

> 10. Lieb and her fellow ICE special agents obtained the Defendant's voluntary consent to enter into the Defendant's home and this consent was secured from the Defendant after Lieb indicated that she wished to speak with the Defendant concerning illegal activity regarding the use of his credit card over the Internet.
>
> ***
>
> 21. As a result of Lieb's failure to discount the Defendant's belief that he was a victim of a crime, Lieb was given the Defendant's voluntary consent to search his computers for evidence that he was indeed a victim of a crime.

Richardson I at 734, 735-736. The voluntariness of the Defendant's consent for the agents to enter his home and search his computers is thus the law of the case. Therefore, the Court focuses its attention on the scope of the resulting consensual search.

B. Scope of the search by consent

Kilpatrick was the agent who performed the forensic analysis of the two hard disc drives. In order to determine if the Defendant was truly the individual who *attempted* access to the child pornography Web site, Kilpatrick began his search by searching for images of child pornography. *See* FOF 43a,43b. It is clear that in this instance, a search for images on the hard disc drives was outside of the scope of the Defendant's consent to search. This search would also be beyond the scope of

[8]Even if it could be concluded that this Court previously ruled upon the issue of scope, the nature of the Court's analysis herein clearly provides one with an understanding that any prior ruling on scope was "clearly erroneous and would create manifest injustice." *In re City of Philadelphia Litigation, supra.*

consent even if Kilpatrick believed that another individual used a potential wireless Internet connection emanating from the Defendant's home.

As recognized in *Richardson I*, the Court did not find a violation of the Fourth Amendment warrant requirement in light of the fact that Lieb believed that the Defendant could have been a victim of identity theft and the vagueness of her description of "credit card activity over the Internet" resulted in a consensual search. *See* FOF 10; *Richardson I* at 735-736. The Defendant and his wife, despite broaching the subject of child pornography, *see* FOF 17, were never told by Lieb that child pornography was the suspicion driving her investigation:

> 14. Lieb embraced the Defendant's view that he was a victim of a crime by failing to reveal her true belief that the Defendant was in fact the person attempting to use his own credit card to illegally obtain child pornography.
>
> 15. Lieb, Rochford or Kilpatrick's failure to reveal the object of their investigation, i.e. an attempted purchase of child pornography over the Internet, did not cause the Defendant's voluntary consent to their entry into his home to be in violation of the *Fourth Amendment*. *See Brown v. Brierley*, 438 F.2d 954, 958 (3d Cir. 1971)("if the police must announce their investigatory intentions even when acting openly in their official capacities, it might well follow that the police also must explain their purposes to criminal suspects when carrying out undercover investigations in which it is necessary that the police camouflage their identity.")

Richardson I at 735. Of course, Lieb, Rochford or Kilpatrick's subjective intent or goals are not the object of scrutiny in analyzing the scope of a voluntary, consensual search:

> The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of 'objective' reasonableness-what would the typical reasonable person have understood by the exchange between the officer and the suspect? The question before us, then, is whether it is reasonable for an officer to consider a suspect's general consent to a search of his car to include consent to examine a paper bag lying on the floor of the car. We think that it is.
>
> ***
>
> We think that it was objectively reasonable for the police to conclude that the general

> consent to search respondent's car included consent to search containers within that car which might bear drugs. A reasonable person may be expected to know that narcotics are generally carried in some form of a container.

Florida v. Jimeno, 500 U.S. 248, 251 (1991)(internal citations omitted). The absence of discussion or mention of child pornography by Lieb, Rochford and Kilpatrick with the Defendant certainly constricts what a reasonable person would believe to be the limits of the search. Excluding images of child pornography from the scope of the agents' search is consistent with the fact that their communications with the Defendant and his wife concerned "['illegal'] credit card activity over the Internet". FOF 31-33. This is the extent of explanation the Richardsons received from the ICE agents.

The Government argues that the understanding of the scope of consent is measured by what the law enforcement officer understands is reasonable. Government's Response, p. 17; Government's "Proposed Findings...." (Document No. 101), pp. 11-12. The Government emphasizes the language referring to what is "reasonable for the police [officer]". *Jimeno* at 251; Government's "Proposed Findings....", pp. 11-12. The Court does not understand *Jimeno* in that way. *Jimeno* sets forth a reasonable person standard which is an objective standard, one in which the "exchange" (as used in *Jimeno* to refer to the statements between the police officer and Jimeno, including the police officer's statements that he suspected Jimeno of possessing "narcotics" in his vehicle and he would be searching for such items) between suspect and police officer is evaluated. *Id.* When reading this quote in context with the preceding sentence this conclusion becomes clear. Understanding this over-arching statement of *Jimeno* that the "exchange" between suspect and police officer is critical, it is clear that a police officer cannot have an"exchange" with himself.

The Court understands the quoted passages from *Jimeno* to impute what is reasonable to a police officer because he has been a participant in the "exchange" and therefore knows what was said. Therefore, what the law understands to be within a reasonable person's mind applies equally to law enforcement and the person granting consent to search based upon their "exchange". As required by *Jimeno*, the "exchange" between the two parties must be evaluated objectively, and subjective knowledge or understanding of the parties plays no part. *See Jimeno* at 251.

With the subject matter of the conversation revolving around illegal credit card usage and Internet activity, a search for images was far afield from the subject matter of what Web sites the computers were used to access. Kilpatrick confirmed that he " was to examine the contents of the two computers that we had consent to search for to find whether or not there was evidence that that credit card had been used from a computer in that house to access child pornography." FOF 43c. The agents knew of two *attempted* entries into the "ILLEGAL.CP" Web site, not two *successful* entries, but this knowledge was not disclosed to the Defendant. FOF 17a, 17b. The Defendant signed two consent forms, Government Exhibits 1 and 2, permitting the Government to search "for evidence of a crime or other violation of the law." The context within which these forms were presented to the Defendant was such that he was not the suspect of the crime, but a possible victim, whose computers contained information that could lead to an identification of the suspect.

Some of the additional findings of fact set forth above address the subject of wardriving, which was not addressed in the hearing on the first motion to suppress. The Government offers wardriving as the potential basis for explaining how a person outside of the Defendant's household could access the Defendant's Internet service in an attempt to access the child pornography Web site without the

Defendant knowing about the two attempts. For wardriving by an individual outside of the Richardson household to be a plausible alternative explanation to the agents' belief that the Defendant attempted the access in question, the Defendant must have possessed a wireless Internet network. The evidence does not indicate that Lieb inquired as to the presence of a wireless network. FOF 17d. Aside from this portion of Lieb's testimony, the remainder of the agents' testimony does not address any inquiry by them to the Richardsons regarding the presence of wireless technology associated with the Richardsons' computers in January and February 2006. The absence of such a wireless network would definitely exclude the potential for wardriving and focus the agents' suspicion upon someone within the household. This failure to inquire of the Richardsons as to the presence of a wireless network at the time of the attempted access bears upon the objective reasonableness of the scope of the search. Had the possibility of wardriving been excluded, suspicion of the criminal attempt would be restricted to those having access to the household computer, the Defendant's email address, telephone number, credit card number and the accompanying cvv number on his credit card. *See* Defendant's Exhibit A.[9] Narrowing the suspicion for the attempted access to certain individuals with access to the Defendant's computer and personal information would place a request to search in a very different light as compared to what did occur in the case *sub judice*. In such a hypothetical situation, the potential suspects for identity theft would be limited only to those who have access to such information and the household computers, which from the record appears to be at least two individuals, the Defendant's wife or

[9]Pursuant to FRE 201 because such facts are "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned", it is judicially noticed that the CVV number (also referred to by other acronyms including a CID number) from a credit card is located on the rear of most credit cards, with the notable exception of the American Express card, which places its number on the front of the credit card.

daughter. If they did not attempt the access, only the Defendant would remain as a suspect.[10] Nevertheless, it has not been proven that questions regarding a wireless Internet network were purposefully avoided by the agents in an effort to obtain a general consent to search without limitation.

In the case *sub judice*, Lieb and the other agents let the vagueness of their reference to "['illegal'] credit card activity over the Internet" permit the Defendant's concern for himself or his wife being a victim of illegal use of their credit card to result in the Defendant's consent to search the two computers for such evidence. Lieb's vagueness in describing what allegedly occurred over the Internet and failure to discount the possibility of wardriving through any questioning of the Richardsons or specific review of Internet related files resulted in the voluntary consent she sought and needed in the absence of a warrant. However, Lieb's vague description also resulted in the unintended restriction of what one could consider was the objectively reasonable scope of the search.

Jimeno teaches that the "[t]he scope of a search is generally defined by its expressed object." *Florida v. Jimeno*, 500 U.S. 248, 251 (1991)(citation omitted). In *Jimeno*, the object was "narcotics", which were found in a bag on the floor of the back seat of a vehicle; oral consent to search was provided by Jimeno after the police officer warned Jimeno that he believed him to be possessing narcotics. *Id.* at 249-250. No limitations upon the scope of the search were otherwise provided by Jimeno. *Id.* at 251. The absence of case law on the issue of the scope of consensual searches (after both oral and written consent) of computers where the consent was obtained using a ruse requires the Court to rely upon *Jimeno* by analogy.

---

[10]It is noted that this hypothetical excludes the remote possibility (not evidenced in the record) of any remote hacking into and commandeering of the Defendant's computer as opposed to his Internet network. *See* S.T., p. 91.

With Lieb's indications that the object of the instant search was "['illegal'] credit card activity over the Internet", a reasonable person under the present circumstances would understand such activity as having been committed by someone other than the Defendant. This is because the testimony and evidence reflect that the agents' words and actions contained no indication to the Defendant that he was a suspect. While it is true that the Defendant made remarks concerning identity theft and that while living in Germany, child pornography was discovered on his former computer that he subsequently gave away, it was the agents' vagueness in their conversation that caused the Richardsons to put forth these suggestions to the agents. The Government's argument in footnote nine of its Response is without merit as the Defendant explicitly told the agents that the child pornography he spoke of was involved in an incident that occurred in the past while he lived in Germany, that he reported it to the authorities and subsequently gave that computer away after removing the child pornography. *See* FOF 17. It could not be reasonably understood that the Defendant's discussion of this previous occurrence gave the agents permission to search for child pornography on the computers he currently owned because the Defendant did not report that he received or discovered any child pornography in the two computers. The agents never stated that their suspicion was that the Defendant's computers contained images of child pornography or that they were searching for any images at all. There is no evidence that the agents mentioned "pornography" or "images" in the conversation of September 6, 2006. The fact that the Defendant made remarks about a computer he previously owned in Germany does not provide a basis for this Court to find that the scope of the consensual search included a search for images. The agents commented about Internet activity, in particular use of the Defendant's credit card, not about child pornography. FOF 17, 17a, 17b, 31, 32, 33, 33a.

The suggestions of the Richardsons, although relevant to the objective standard, are by their nature subjective in that they were a personal reaction to the vagueness of the agents' explanation. In particular, there was no evidence that the topic of child pornography mentioned by the Richardsons was confirmed by the agents to be the object of the instant search of the computers. The Richardsons' suggestion of alternatives such as discrepancies in their credit card statements, child pornography on their former computer or a telemarketer who possibly stole their identities indicate that the Richardsons were not being told by the agents what they were specifically looking for in terms of illegal use of a credit card over the Internet. If the Richardsons had to keep suggesting alternatives, it is clear from the record that the agents were being vague in their explanation and their request to search. Moreover, their offering of suggestions reflects that the Richardsons were not being told by the agents that any of the suggestions were indeed the object of their investigation and their subsequent search. The Richardsons' suggestions of alternatives appear to have been made in an attempt to understand the agents' remarks about the use of their credit card on the Internet and thereby reflect the Defendant and his wife's lack of understanding of what the agents were attempting to investigate and search out. The continued suggestion of explanations to the agents cannot be found to expand the scope of a subsequent search because those fears were voiced by the Richardsons while the agents in effect sat idly by and failed to confirm or deny any suggestion. If Lieb, Rochford or Kilpatrick had explicitly confirmed that the credit card activity concerned the purchase of child pornography, it would be unquestionable that any consent to search given after that would permit a search for such images. The record is devoid of any such remarks made by the agents. If there is no meeting of minds on the subject matter of the search between the person seeking consent to search and the person granting consent to search, the consent to search

cannot be found to authorize a search for any subject matter because the Defendant objectively lacks understanding of what the Government is seeking.

Additionally, any unvoiced suspicions or thoughts of the agents that the Defendant possessed child pornography or the Defendant's thoughts that the agents were present to search for child pornography, *see* FOF 68, are subjective and were not part of the "exchange" between the Defendant and the agents. Therefore, any disjunction between the thoughts of the Defendant and the agents cannot be considered when applying *Jimeno* to the facts of the case *sub judice*.

Now having observed what was said and not said by the parties, the Court proceeds to evaluate the scope of the search based upon the actual exchange between the parties. First, a better understanding of how computers retain information regarding their use on the Internet is necessary to evaluate the scope of the Defendant's consent.

Personal computers used to access the Internet catalogue their Internet usage through more than one type of file stored on the computer's hard disc drive. One manner in which a computer stores Internet activity is through the computer's Web browser which caches the Web pages and their images that are accessed. Eoghan Casey, *Digital Evidence and Computer Crime* 279 (2d ed. 2004).[11] Web pages that are stored in cache indicate "creation and modification times [that] are the same time as the page was viewed. When the same site is accessed in the future, the cached file is accessed." *Id.* In the separate browser history file, the computer catalogues the number of times a Web page was accessed

[11]Pursuant to its discretion provided for in Federal Rule of Evidence 201, the Court takes judicial notice of this and the proceeding facts of this paragraph regarding the files of personal computers that contain evidence and traces of Internet activity as such facts are "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned" and the Court finds that the cited text is such a source. Fed. R. Evid. 201.

by the computer. *Id.* Two Internet browsers, Netscape and Internet Explorer, catalogue the names of Web sites the browsers visited in files named "netscape.hst." and "index.dat." respectively. *Id.* Another manner of tracking Internet habits is through a Web site's use of a type of file generally referred to as a "cookie" which catalogues one's visits to the Web site; the cookie file is placed onto the computer accessing the Web site. *Id.* at 280.[12]

"Government agents may not obtain consent to search on the representation that they intend to look only for certain specified items and subsequently use that consent as a license to conduct a general exploratory search." *United States v. Dichiarinte*, 445 F.2d 126, 129 (7th Cir. 1971); *see also Graves v. Beto*, 424 F.2d 524, 525 (5th Cir. 1970) ("[Graves'] consent, based on the police chief's representations, gave no more than the license that Schmerber provided without his consent. To endow it with wider effect would allow the state to secure by stratagem what the fourth amendment requires a warrant to produce.")(footnotes omitted). After completion of the Forensic ToolKit's analysis of the Defendant's hard disc drives, Kilpatrick reviewed his results for images, not Internet usage. FOF 43a. The Court finds that Kilpatrick's initial act of searching the ForensicToolKit's results for images of child pornography to confirm that the Defendant was the individual who *attempted* the two failed instances of access "ILLEGAL.CP" is not only illogical (considering the fact it was known that the Web site was not accessed), but more importantly it was outside of the scope of the consented search. If the

[12]Cookies cannot always confirm an intent to visit a Web page, including in those instances where advertisements for a Web page included on the Web page being viewed place a cookie from the advertised Web page despite the fact it was not accessed. It is also recognized that "a Web browser may be automatically redirected to multiple sites, creating files in disk cache and entries in the history database even though the user did not intend to visit any of the sites." Casey, *supra*, at 280. Since no review of the Defendant's computer files for cookie files, Web browser cache, or Web browser history occurred in the case *sub judice*, the issue of intent of the Defendant to visit Web pages traced in his computers' hard disc drives is not present.

attempts were unsuccessful as Lieb herself indicated, looking for images downloaded from a Web site that was never accessed would not only appear to be unfruitful, but also irrelevant for purposes of the investigation. The information that would prove the attempted access of the child pornography Web site could be culled from different files, including the Web browser cache, Web browser history or cookie files which catalogue Internet activity as described above.

Images downloaded from the Internet were never a subject addressed with the Richardsons by Lieb or the other agents. However, Web browser history or Web browser cache files as well as cookie files placed on the computer's hard disc drive after visiting a Web site would present the evidence of Internet activity that the agents referenced to the Defendant. There is no evidence of record that these types of files were retrieved or even reviewed by Kilpatrick. Therefore, Kilpatrick's search that focused upon uncovering images of child pornography from the results of Forensic ToolKit's analysis of the Defendant's hard disc drives was beyond the scope of the search to which the Defendant voluntarily consented. Had Kilpatrick searched the results for Web browser cache files, Web browser history files or cookie files, he would have been within the scope of the consent to search given by the Defendant.

A "plain view" argument for discovery of the child pornography also fails because the consented search was limited to a concern for the "['illegal'] credit card activity over the Internet", not images. The image files were not understood to be the types of files to be opened and thus a search of image files was beyond the scope of the consented search and outside of Kilpatrick's plain view. *See United*

States v. Carey, 172 F.3d 1268, 1272-1274 (10th Cir. 1999).[13] In sum, the "plain view" argument fails because Kilpatrick was within computer files he was not permitted to be in when he viewed the images.

Moreover, even if the Defendant was made aware of the extent of the information that Lieb and the agents possessed as a result of Operation Emissary, the immediate search for images would still be a search for evidence of a separate crime committed by someone who not only was successful in downloading child pornography but who also had access to the Richardsons' computers and not a crime committed by someone wardriving for wireless Internet signals outside of the Richardson home. Therefore, if on September 6, 2006 the agents made the Richardsons aware of the attempted access to "ILLEGAL.CP" and if the same voluntary consent to search was given by the Defendant, conducting a search of the hard disc drives for images would still have been beyond the scope of the voluntary consent to search.

Additionally, the presence of child pornography on the computers could have just as easily occurred through the saving of the images onto the hard disc drive through a transfer of images from another storage medium unrelated to the Internet. The presence of images of child pornography does not justify the conclusion that these images were downloaded from the Internet onto the Defendant's hard disc drives. In turn, any mention of "['illegal'] credit card activity over the Internet" by the agents cannot be objectively understood to include a search for images of child pornography.[14]

---

[13]It is recognized that the *Carey* court limited its holding to the facts before it. *Carey* at 1276.

[14]Even if the agents had searched for any credit card activity over the Internet, and it were assumed that this meant that it included the purchase of images of child pornography using a credit card, it cannot be assumed that this would include all possible child pornography images as the Court understands that not all child pornography downloaded from the Internet is purchased, but it is also readily obtained without purchase including through trading or bartering of images between those members of peer to peer networks who possess such images.

As a result, not only did the agents fail to adhere to searching the Internet activity of the computers seized as discussed with the Defendant, but they also failed to adhere to the parameters of their own suspicions as testified to in the supplemental evidentiary hearing, specifically in their suggestion that wardriving was a possible explanation of the evidence received from Newark ICE. This is evident by the agents' failure to investigate the presence of a wireless modem on September 6, 2006, their failure to question the Richardsons regarding their use of a wireless modem during January and February 2006 and Kilpatrick's pointed search for images of child pornography on the hard disc drives, without searching for information regarding Internet activity, when they were aware the two attempts to access "ILLEGAL.CP" had failed.

Professor LaFave best characterizes the nature of the agents' unconstitutional search:

> Another type of case is that in which the police mislead the consenting party as to the nature of the crime under investigation and, consequently, the character of the objects for which they desire to conduct a search. Assume, for example, that the police indicate a desire to search a suspect's premises for narcotics and the suspect, knowing he has no narcotics, consents to such a search, during which the police pursue their undisclosed purpose of opening and examining certain documents. This is a relatively easy situation with which to deal, for it is clear that police "may not obtain consent to search on the representation that they intend to look only for certain specified items and subsequently use that consent as a license to conduct a general exploratory search." But, the fundamental point here is that a search pursuant to consent may not be more intensive than was contemplated by the giving of the consent; a search for narcotics does not require an examination of documents, and thus this examination would be illegal even if the police had been speaking the truth when they said at the time of soliciting the consent that their present intention was only to search for narcotics.

4 Wayne R. LaFave, *Search & Seizure* § 8.2 (4th ed. 2008)(footnotes omitted).

The record reveals that Kilpatrick's search for images was made after the agents approached the Richardson household in order to gather information as to whether the Defendant *attempted* to access

the Web site or someone else *attempted* to access the Web site using his identity. It is clear from the record that a search for images of child pornography is unrelated to a search for criminal evidence of *two failed attempts* to purchase child pornography. Such a search for images contradicts the testimony of Kilpatrick that wardriving was a possible explanation for the *two failed attempts* to access "ILLEGAL.CP". The possibility that wardriving resulted in the two failed attempts could not be confirmed or discounted by a search for images.

Quite simply, the agents in the case *sub judice* made an assumption that the Defendant's computers would contain child pornography because the evidence from Operation Emissary indicated that the Defendant made two failed attempts to access "ILLEGAL.CP". Their assumption proved correct, but only after consent to search the computers was obtained in order to look for evidence of unspecified "['illegal'] credit card activity over the Internet", not images of child pornography or any images for that matter. Kilpatrick did not look for catalogued evidence of Internet activity as stored upon the two personal computers. Kilpatrick searched for images, images that could not have been on the computers as a result of the two known failed attempts to access a child pornography Web site. These failed attempts were the basis for the agents' vague and unspecified Internet activity described to the Defendant and his wife. The search for images proceeded to look for evidence of another instance of crime different from the failed attempts to access the "ILLEGAL.CP" Web site. The search that was conducted was not only outside of the scope permitted by the Defendant, but also outside of the scope of what the agents were aware of after a review of the evidence received from Newark ICE.

The Court's previous opinion recognized that the possible explanation for the two failed attempts to access "ILLEGAL.CP" was the possibility that the Defendant was a victim of a crime and

thus the Defendant's consents were voluntarily made. *Richardson I* at 728, Conclusion of Law (COL) 21. Nothing in Kilpatrick's actions to find images of child pornography vitiates the fact that the Defendant gave voluntary consent to search, but it was a search limited in scope to Internet activity. A search for images of child pornography is beyond the scope of the vagaries of the "['illegal'] credit card activity over the Internet" and seeks one thing, the presence of child pornography that the agents knew was not related to the information of the January and February 2006 attempts presented to Lieb by ICE Newark. This search for images was beyond the scope of the consent granted. Searching for images of child pornography relates to a separate crime, one unrelated to the ruse which was presented and for which the ruse did not provide a basis for the consensual search. Lieb and the other agents thus used the vagueness of their request based upon evidence of an undisclosed, attempted crime to obtain a voluntary consent in order to search for evidence of a separate crime, one for which they did not believe the Defendant was a victim, but in fact the sole perpetrator. The search for images of child pornography was far afield from the voluntary consent to search for evidence of "['illegal'] credit card activity over the Internet", activity which unbeknownst to the Defendant was the two failed attempts to purchase access to the "ILLEGAL.CP" Web site.

Therefore, because the ICE agents searched for matters beyond the scope of the consensual search, the images of child pornography revealed from the forensic examinations of all computer equipment seized or imaged and obtained must be suppressed as being beyond the scope of the oral and written voluntary consent granted by the Defendant.[15]

---

[15]The Court notes the following sentence is set forth in the Conclusion section of the Memorandum Opinion in *United States v. Richardson*, 501 F.Supp.2d 724, 738 (W.D.Pa. August 3, 2007): "The ruse was a permissible tool to...subsequently search these articles because the ICE agents were obtaining a view of matters that one would view if they

The Court recognizes the Government's argument that the Defendant granted both oral and written consent to search and that in particular the written consent provided was not limited in any way by the Defendant. Government's Response, pp. 19-20. Government Exhibits 1 and 2 certainly do not limit in their express language the search of the computers listed to any certain file or to a particular user's files. However, if the Court were to read the written consents to search as permitting an unrestricted search of the Defendant's computers, such unrestricted searches of the computers would be inconsistent with the original oral consent that was obtained after a discussion of "['illegal'] credit card activity over the Internet" but prior to signature of the consent forms. The Court cannot find any basis to conclude that an oral voluntary consent to search two computers for "[illegal] credit card activity over the Internet" can somehow be expanded to a general exploratory search by the mere memorialization of consent in a preprinted form. If law enforcement were permitted such an expansion of the scope of a consensual search by the memorialization of an oral consent that was limited in scope and granted prior to the written consent, law enforcement could always avoid limitations of the scope of consensual searches by providing a preprinted consent form that is not subject to limitation.

Lieb, Rochford and Kilpatrick presented the Defendant with a concern of the presence of a crime concerning his credit card being used on the Internet. This was the object of their search. Knowing this to be the object of the requested search, oral consent to search the Defendant's computers

---

were investigating a possible theft of one's identity over the Internet." To the extent that this sentence suggests that the ICE agents, particularly Kilpatrick, adhered to the scope of the consent granted by the Defendant, this sentence was a summary of the findings and conclusions of the Court on this matter after no objection was raised regarding the scope of Kilpatrick's search. No finding of fact or conclusion of law was made in *Richardson I* regarding the scope of Kilpatrick's search. In fact, the actual scope of Kilpatrick's search was never factually addressed in *Richardson I*. To the extent it would be considered a previous ruling upon the scope of the search, it is overruled by today's analysis and conclusion in light of the new and additional evidence presented regarding the details of Kilpatrick's search and analysis of the content of the computers.

was granted. Kilpatrick filled in the computer information on the pre-printed forms at Government Exhibits 1 and 2, and the Defendant signed these forms while being presented with a concern for the security of one of his credit card accounts; he was lead to believe the agents were helping him as a victim. To allow the use of a pre-printed form to exorcize the limitations the agents presented in their vague description of the object of their search would stand the goal of cooperation through consensual searches on its head. No private citizen could trust law enforcement if such a bait and switch scheme were permitted under the Fourth Amendment. Consensual searches would become less frequent for the mistrust that is typically reserved to attorneys for their use of exceptions in the fine print of documents would quickly spread to the requests for signatures on consent forms provided by law enforcement.

The agents' vague representation regarding credit card activity being transacted over the Internet was the object of their search they chose to indicate to the Defendant. They chose not to indicate that they aspired to search his computers for images of child pornography. The vague object imparted upon the Defendant a concern for being a victim, not a suspect, and in this mindset, the words of Government Exhibits 1 and 2 must be read, that is through the objective understanding given the conversation between the Defendant and the agents. The presence of a written consent without express limitation does not save the Government from the limitation they made upon the consensual search through their voicing of the object of the search. *Cf. United States v. Miller*, 450 F.Supp.2d 1321 (M.D.Fla. Aug. 28, 2006)(police officers obtained consent to search "computer" for child pornography where the word "computer" was added to the consent form and scope of consent was understood to include the defendant's CPU tower as well as an attached external hard drive because of the Defendant's

explanation of his computer components and their use given prior to his oral and written consent to search); *United States v. Brooks*, 427 F.3d 1246 (10th Cir. 2005)(explicit written consent to search CPU tower for images of child pornography in a "pre-search" did not restrict the method of a "pre-search", whether through operation of a software program or through a manual search of image files by a Government agent).

As *Miller* and *Brooks* indicate, the context of the consent is critical as all consents to search are not the same. Additionally, not all written consents that are executed can contain a written explanation of the minutia of descriptions for each object sought or every action to be taken in furtherance of the consented search. Therefore, pre-printed forms within which a description of the item to be searched can be inserted and which also state (as do Government Exhibits 1 and 2) that the consented search is "for any evidence of a crime or other violation of the law" cannot be assumed to change the scope of a consented search when the scope requested and/or discussed orally prior to providing written consent is reasonably understood to be otherwise. This is consistent with the holding in *Jimeno* as it requires that an objective review be taken of the "the exchange between the officer and the suspect". *Florida v. Jimeno*, 500 U.S. 248, 251(1991). Some exchanges regarding consent to search may only be oral, some exchanges may only be written, but the case *sub judice* has evidence of both and the Court cannot ignore the oral evidence and focus upon the written consents. The Court is guided by the Fourth Amendment and the controlling precedent in *Jimeno*, not by the parol-evidence rule.[16]

---

[16]The parol-evidence rule is defined in relevant part by Black's Law Dictionary as "[t]he common-law principle that a writing intended by the parties to be a final embodiment of their agreement cannot be modified by evidence of earlier or contemporaneous agreements that might add to, vary, or contradict the writing." *Black's Law Dictionary* 1149 (8th ed. 2004).

This Court is not alone in this understanding of *Jimeno*. Judge Baldock of the Tenth Circuit Court of Appeals penned a concurrence in *United States v. Carey*, 172 F.3d 1268, 1277 (10th Cir. 1999) that echoes this Court's holding today. In *Carey*, the defendant was arrested pursuant to a warrant for distribution of controlled substances, but the police officers' plain view of his residence during the arrest revealed marijuana and related paraphernalia. *Carey* at 1270. The police officers requested consent to search and indicated that if no consent was given, a search warrant would be obtained; the defendant withheld consent to search until he was brought to the police station at which time he signed a written consent. *Id.* After consent was given by the Defendant, the police returned to his residence to conduct a search and during the search seized two computers, which were taken to the police station for a search of matters "pertaining to the sale and distribution of controlled substances" pursuant to later-obtained search warrant. *Id.* A search of the computers uncovered child pornography, which was suppressed because the police officers ceased looking for material under the search warrant related to controlled substances and began an independent search for more child pornography on the computers. *Id.* at 1271, 1273. Explaining his reason for joining the majority in the conclusion that the scope of the original consent to search the residence was confined to "drugs and drug-related items in the apartment", Judge Baldock wrote:

> Second, while agreeing with the majority that Defendant's consent to the search of his apartment did not carry over to his computer hard drive, I write separately to explain why I think the scope of Defendant's consent is limited to evidence of drug-related activity. The scope of a consensual search is "generally defined by its expressed object." *Florida v. Jimeno*, 500 U.S. 248, 251, 114 L. Ed. 2d 297, 111 S. Ct. 1801 (1991). To determine the breadth of the consent given by Mr. Carey, we consider what "the typical reasonable person would have understood by the exchange between the officer and the [defendant]." *United States v. Elliott*, 107 F.3d 810, 815 (10th Cir. 1997). Resolution of this issue requires a detailed inquiry into the facts.

> The waiver signed by Defendant granted the officers permission to search the "premises and property located at 3255 Canterbury # 10" and authorized the officers to remove any property "if said property shall be essential in the proof of the commission of any crime . . . ." The officer testified that after he arrested Defendant, he told him that "based on what I had just observed in his apartment that I was going to apply for a search warrant." The officer had just found, in plain view, a bong typically used for smoking marijuana and a small quantity of what appeared to be marijuana. The officer then explained to Defendant that he could consent to a search instead of the officer obtaining a warrant. Defendant told the officer he was unsure. En route to the police station, Defendant asked several questions about the search. Upon arrival at the station, Defendant indicated that he wished to consent. He also told the officer where he would find additional drugs, a scale, a firearm and cash. In addition, Defendant told him where he would find a pornographic videotape. The officer responded that he "couldn't care less about his pornographic videotapes" and "that wasn't of concern to me."
>
> In light of the officer's conversations with Defendant, a reasonable person would conclude that the statements by the officer limited the scope of the request to drugs and drug-related items in the apartment. *See Elliott*, 107 F.3d at 815; *see also, United States v. Dichiarinte*, 445 F.2d 126, 129 (7th Cir. 1971) (consent to search after officers repeated references to narcotics did not grant officers a license to conduct a general exploratory search). As in *United States v. Turner*, 169 F.3d 84, 1999 U.S. App. LEXIS 3131, 1999 WL 90209 (1st Cir. 1999), the Defendant's consent did not include permission to search the hard drive of Defendant's computer for pornographic or any other type of files, a fact, as the majority points out, the officer recognized because he obtained a proper warrant to search for drug-related evidence before he began opening computer files. Thus, I think the record supports a finding that Defendant's consent did not extend to a search for pornographic material on the hard drive of his computer. Of course, the officer's search of the computer hard drive for "evidence pertaining to the sale and distribution of controlled substances" was lawful, in that the officer obtained a valid search warrant to do so.

Carey at 1277. The "exchange" between the police officer and the individual from whom he seeks consent to search is critical to understanding the scope of the police officer's search, whether consented to orally and/or in written form. It is clear that Judge Baldock believed that in light of the conversations between Carey and his arresting police officers, Carey's consent to search was limited to arena of controlled substances and related paraphernalia despite the presence of the words "in the proof of the

commission of any crime" on the written consent form.

In the case *sub judice*, the Defendant was not told, nor was it or otherwise made known to him that he was a potential suspect. Therefore, it was objectively reasonable for him to read the words "for any evidence of a crime or other violation of the law" on the forms at Government Exhibits 1 and 2 to mean that Lieb, Rochford and Kilpatrick believed he was a victim and the search was to be for items related to "['illegal'] credit card activity over the Internet", not a search for images stored on his computer.

C. Taint and the Defendants' Statements

Having concluded that all of the images are to be suppressed, the Court now reviews the impact this illegally seized evidence had upon the progression of the investigation of the Defendant. The Defendant arrived at the ICE office in Pittsburgh, Pennsylvania on September 22, 2006 after two or three telephone conversations with Lieb that occurred after Lieb's September 6, 2006 visit to the Richardsons' home. *See* FOF 45, 46. This Court has already concluded that the Defendant was not in custody during the two meetings between the Defendant and Lieb that took place on September 22, 2006. *See Richardson I* at 737, COL 34-36. The Court also concluded that Lieb's request of the Defendant to bring the actual Hewlett Packard hard disc drive was improper and ordered its exclusion from evidence at trial. *Id.* at 736, COL 29. After today's conclusion that Kilpatrick went beyond the scope of the consensual search permitted by the Defendant resulting in the suppression of the images obtained from the "image" of the Hewlett Packard computer[17] and the hard disc drive of the Nascar PC

[17]In *Richardson I*, the Court excluded from introduction into evidence the actual Hewlett Packard computer including its hard disc drive obtained by Lieb on September 22, 2006, but not the "image" of that same hard disc drive obtained on September 6, 2006. *Richardson I* at 736.

by CISNET, the Court must evaluate if the Defendant's statements to Lieb are tainted by the illegal search. The Court concludes that all of the Defendant's statements made to Lieb on September 22, 2006 are in fact tainted by the illegal search of the Defendant's computers.

"The exclusionary prohibition extends as well to the indirect as the direct products of ['an unlawful search']." *Wong Sun v. United States*, 371 U.S. 471, 484-485 (1963)(citation omitted). "Thus, verbal evidence which derives so immediately from an unlawful entry and an unauthorized arrest as the officers' action in the present case is no less the 'fruit' of official illegality than the more common tangible fruits of the unwarranted intrusion." *Wong Sun* at 485-486 (footnote and citation omitted). Recently, the Supreme Court in *Hudson v. Michigan*, 547 U.S. 586, 591 (2006) noted that the exclusionary rule is truly a "last resort," one in which the need for remediation of the present actions as well as the deterrence of future actions of the Government's agents overcome the concern for permitting those culpable to be in effect relinquished from prosecution. *Hudson* recognized that the exclusion of evidence does not solely rest upon the fact that it was developed but for the violation of the Fourth Amendment but that if "but-for" causation exists, the next consideration is if the fruits of the illegal search are sufficiently attenuated from the illegal search to be purged of any taint. *See id.* at 592-593. "Attenuation can occur, of course, when the causal connection is remote. *See, e.g., Nardone v. United States*, 308 U.S. 338, 341, 60 S.Ct. 266, 84 L.Ed. 307 (1939). Attenuation also occurs when, even given a direct causal connection, the interest protected by the constitutional guarantee that has been violated would not be served by suppression of the evidence obtained." *Id.* at 593.

Lieb's request for the Defendant to come to Pittsburgh and speak with her on September 22, 2006 came after discovery of images by Kilpatrick. As soon as the Defendant arrived and gave Lieb the Hewlett Packard hard disc drive, Lieb confronted him with Kilpatrick's discovery of the images and began to question the Defendant regarding them. The Defendant gave two statements that day regarding the images found. No discussion regarding "['illegal'] credit card activity" occurred, despite the fact that the Defendant was lead to believe that Lieb was still investigating such an occurrence up to the time of his relinquishing of the hard disc drive. After the transfer of possession of the Hewlett Packard hard disc drive, Lieb revealed her true inquiry of the Defendant. Lieb's questioning of the Defendant regarding the images of child pornography did not occur at the time of the initial encounter at the Defendant's residence because Kilpatrick sought to image the hard disc drives of the computers, not preview their contents. Only after review of the discs' contents could Lieb approach the Defendant regarding the presence of the images of child pornography. It was Kilpatrick's search for images that lead to the Fourth Amendment violation. Lieb's invitation to the Defendant to come to her Pittsburgh office was prompted by the discovery of the images. Her continued implementation of the "ruse" regarding identity theft up to the time of the Defendant's arrival not only reveals that the September 22nd questioning of the Defendant and his resulting statements were the result of the discovery of the images of child pornography, but that the questioning of the Defendant regarding the images is not purged of any taint because of the lack of attenuation from the illegal search.

Suppression of these statements serves the purpose of the Fourth Amendment in that the consensual search took place away from the Defendant's home, while the imaged drive and the Nascar PC were in the possession of the Government. The review of their contents uncovered evidence of a

crime, but that review was beyond the scope of the search permitted by the Defendant imposed before the imaged drive and Nascar PC left his home. Unlike the instance of *New York v. Harris*, 495 U.S. 14 (1990) where the defendant's illegal arrest and his statement to the police in the home were suppressed, but his later statement made at the police station was not because of sufficient attenuation from the Fourth Amendment violation, the case *sub judice* concerns a consensual search performed outside of the Defendant's home at the ICE office, the scope of which was violated by agents' actions at the ICE office, and the Defendant was subsequently requested to present himself at the ICE office and surprisingly questioned regarding the images revealed in the illegal search.

Kilpatrick's search relied upon the consent of the Defendant because of the absence of a warrant. He then searched the contents of the two hard disc drives in a manner that was beyond the scope of the consent. Kilpatrick did this by searching for image files, not files that reflect the computer's Internet activity. The fruits of that search were the basis of Lieb's questioning of the Defendant who was not told of the discovery of the images until he was present at the ICE office. Without a search that extended beyond the permitted scope of the Defendant's consent, the images would not have been discovered and could not have been the subject of any discussion between Lieb and the Defendant. The images' discovery is not only the "but-for" cause of the Defendant's statements, but reference to such images is so closely related to the resulting statements of the Defendant that exclusion of the images without exclusion of the Defendant's statements would frustrate the exclusionary rule. There would have been no basis to invite the Defendant to the ICE office and commence any conversation regarding child pornography images without the scope of the Defendant's

consent having been violated.[18] To allow the use of the Defendant's resulting statements would permit the Government to avoid today's suppression order as if no illegality occurred.[19] Statements with similar connection to evidence uncovered have been suppressed under different circumstances. *See United States v. Davis*, 332 F.3d 1163 (9th Cir. 2003)(excluding statements made as a result of an illegally seized firearm because statements were fruit of poisonous tree) ; *but see United States v. Marasco*, 487 F.3d 543, 547-548 (8th Cir. 2007)(no demonstration that illegal search was "but-for cause of...statements") and *United States v. Schecter*, 717 F.2d 864, 871 (3d Cir. 1983)(search found to be legal, thus no poisonous tree existed).

Therefore, the Court will grant that portion of the Defendant's motion seeking exclusion of all of the Defendant's statements made on September 22, 2006 as being tainted by the illegally obtained images of child pornography. The Court finds no basis to revisit its previous determination that no *Miranda* violation occurred with regard to the Defendant's statements of September 22, 2006 because he was not in custody. *See Richardson I* at 737, COL 36.[20]

---

[18]To compound the violation, although it is not entirely clear from the record, it appears that in each of the two or three conversations Lieb had with the Defendant after September 6 but before September 22 no mention was made of the discovery of the child pornography and the "ruse" was continued by Lieb. *See* FOF 45-47. It is clear from the record that Lieb's final telephone conversation is when she requested that the Defendant come to her office and bring the Hewlett Packard computer. *Richardson I,* p. 736, COL 26-29.

[19]Of course, admission of the statements would be subject to the application of the *corpus delicti* rule. *See Wong Sun v. United States*, 371 U.S. 471, 488-490 (1963); *United States v. Opdahl*, 610 F.2d 490 (8th Cir. 1979).

[20]Conclusion of Law 36 indicated that the Defendant was not in custody and his statements of September 22 were also not "fruit of the poisonous tree", *Richardson I* at 737, but this latter conclusion, as mentioned earlier, resulted from the *Richardson I* analysis that centered upon the voluntariness of the Defendant's consent, not the scope of his consent. Today's conclusion regarding taint evolves from the search by Kilpatrick beyond the scope of consent.

The Court finds no basis for exclusion of any statements made by the Defendant on September 6, 2006 when Lieb, Rochford and Kilpatrick came into the Defendant's home and sought permission to search his computers for evidence of identity theft. The Defendant made no statements that day that were ever tainted by the illegal search because Kilpatrick's search of the computer hard disc drives occurred after the three agents left the Defendant's home. Otherwise, the agents' entry into the Defendant's home on September 6, 2006 was made with the Defendant's consent. *Richardson I* at 734, COL 10. The findings of fact do not allow for the conclusion that the Defendant was in custody at any time on September 6, 2006. Finally, no challenges have been made to any statements made in the telephone conversations between the Defendant and Lieb after September 6, 2006 and before September 22, 2006 and no ruling is necessary on this issue.

An appropriate Order follows.

AND NOW, this 31st day of October, in accordance with the foregoing Memorandum Opinion, IT IS HEREBY ORDERED THAT the Defendant's Supplemental Motion to Suppress Evidence Obtained as a Result of an Unlawful Search and Seizure with Accompanying Citation of Authority (Document No. 83) is GRANTED IN PART in that any images discovered from the consensual search of the image of the Defendant's Hewlett Packard computer and the Defendant's Nascar PC by CISNET computer and the same shall be excluded from introduction into evidence in the Government's case-in-chief at the time of trial; GRANTED IN PART as to any statements made by the Defendant to ICE agents on September 22, 2006 and the same shall be excluded from introduction into evidence in the Government's case-in-chief at the time of trial; DENIED IN PART as to all remaining arguments.

BY THE COURT:

KIM R. GIBSON,
UNITED STATES DISTRICT JUDGE